

SAS / ESC APPLICANT MEETING

JULY 18, 2016

Introduction / Agenda

- Purpose: this meeting is intended to be an informal discussion where FCC staff provides guidance on issues that affect most or all applications. We will do our best to answer questions.
- Status: FCC staff, in coordination with NTIA/DOD, have reviewed all of the applications and will be transmitting specific requests for supplemental information to each applicant in the coming weeks.
- Agenda: We will walk through each global issue within a set time frame, including time for questions on each issue.
- This presentation will be publicly available in ECFS, GN Docket No. 15-319

DISCUSSION TOPICS

- PROPAGATION MODELS
- SAS ISSUES
 - Compliance after Software Changes
 - Interference Reports from Incumbents
 - Secondary Markets
 - International Agreements
- SAS-ESC COMMUNICATION INTERFACE
- ESC ISSUES
 - ESC Operational Security
 - ESC Hardware and Information Retention
- SAS-SAS INFORMATION EXCHANGE

Propagation Models

- R&O's Require
 - A common set of propagation models be used by each SAS to ensure consistent protection for all PALs and incumbents.
 - Common calculation across all SASs for determining PAL default protection contour.
- We are encouraged by ongoing industry harmonization efforts to develop a common set of models.
- Testing of SASs will be based on a single model to ensure consistency and accuracy with expected correct outcome.
- The initial model to be used for implementation and testing may evolve in future, e.g. more accurate modelling of clutters and use of measured data.

Compliance after Software Changes

- The PN (DA 15-1426) requested description of methods used to modify software and firmware and address security vulnerabilities:
 - Describe how RF spectrum parameters and spectrum authorizations are retained or (re)established between SAS-CBSDs after software is modified.
 - How SAS ensures that initial and renewed security associations (e.g., private key verification with FCC ID number) are established when CBSD software / data is changed.

Procedure for Responding to Interference Complaints

- Under our rules, an SAS is required to receive reports of interference and requests for additional protection from incumbents.
- Federal Incumbent Protection
 - Process of determining solution still underway (these procedures to be developed by NTIA and FCC).
 - Applicants may provide clarification regarding how they intend to comply with this requirement, to the extent that their solution has been developed.
- FSS Earth Station Protection
 - Applicants need to provide more specific procedure and detailed mechanics to demonstrate compliance with our rules.

Secondary Markets

- The 2nd R&O established a light-touch leasing regime, which SAS Administrators are not required to offer, but if they choose to, must meet the requirements.
 - Lessee pre-certification verification.
 - The lease will not violate the 40 MHz Priority Access Licensee spectrum cap for the given geographic area.
 - Confirmation of notification receipt to licensee.
 - The lease area is within the licensee's Service Area but outside of its PAL Protection Area.
- If applicant intends to offer leasing immediately, paper proposals must demonstrate this completely.
- If applicant intends to offer leasing in the future, applicant must amend proposal to include such demonstration.

International Agreements

- All SAS applicants must affirmatively acknowledge that CBRS operation in the 3550-3700 MHz band is subject to current and future international agreements with Mexico and Canada and that they will implement the terms of these agreements.
- All SAS applicants are responsible for keeping up-to-date on the status and existence of relevant international agreements.
 - We will notify applicants and Administrators of new or changes to agreements.
- The Commission makes all of its international agreements public: <https://www.fcc.gov/general/international-agreements>.
- Agreements between the U.S. and Canada*:
 - **3550-3650 MHz Band:** *Exchange Of Notes Of October 24, 1962 Between The Government Of Canada And The Government Of The United States Of America Constituting An Agreement For Radio Frequency Coordination And Use Of Radio Frequencies Above Thirty Megacycles Per Second*, <https://transition.fcc.gov/ib/sand/agree/files/can-nb/above30r.pdf>.
 - **3650-3700 MHz Band:** *Arrangement R: Sharing Arrangement between the Department of Industry of Canada and the Federal Communications Commission of the United States of America Concerning the Use of the Frequency Band 3650 to 3700 MHz by the Fixed and Mobile Services Along the Canada-United States Border*, https://transition.fcc.gov/ib/sand/agree/files/can-nb/Arrangement_R.pdf.

[*Currently, there is no U.S.-Mexico agreement that specifically addresses frequencies in the 3.5 GHz Band but SAS Administrators must comply with all relevant international agreements]

SAS-ESC Communications Interface

- R&O defines distinct sets of rules for SASs and ESCs which will be the basis for our testing and authorization.
- While some current applicants have proposed to offer SAS-only or ESC-only solutions, most current applicants plan to offer both.
- SAS-ESC interface may or may not be standardized by multi-stakeholders.
- In case of applicants who plan to offer both SAS and ESC functions:
 - They need to provide testing interfaces to ensure all ESC and SAS requirements testing can be conducted.
- SAS-only and ESC-only applicants who apply for operation in Phase 2 need to describe and demonstrate how they work with an ESC or a SAS operator. This is needed so they can be tested for end-to-end interoperability for authorization to operate in Phase 2.

ESC Operational Security

- ESC's should not store information obtained about federal incumbent use and must obfuscate such information when communicating with associated SASs.
- DoD-NTIA may provide additional guidance on ESC configurations to protect OPSEC.
- Requirements apply regardless of whether there is a standard SAS-ESC interface.
- In ESC-SAS combined applications, the proposal should clearly demonstrate how federal stations are protected.
- All SAS-ESC communication protocols, standards based or proprietary, will be tested against security threats.

ESC Hardware and Information Retention

- 24 x 7 Operations required: Provide more information on how ESC will meet this requirement.
- Describe the information to be collected and information to be relayed from ESC to SAS(s).
- When defining the procedure to detect and obfuscate radar location information, describe how applicant will comply with information retention requirements.
- ESC applicants must describe sensor sensitivity, received signal threshold, and resiliency to front-end saturations and burn-out. This should include info on impact of CBSDs on ESC noise floor and false alarm.
- Information on upgradability of ESC to the future radars and applicability of ESC to ground-based radar systems.

SAS-to-SAS Information Exchange

- The Commission has established rules and a processes that significantly favor and encourage industry collaboration versus prescriptive Commission action.
- The rules require that:
 - SASs are to maintain current information on registered CBSDs, including licensee identification, geo-location, assigned channels, maximum power level, and (for Category B CBSDs) antenna configuration.
 - SAS Administrators must make all information necessary to effectively coordinate operations between and among CBSDs available to other SAS Administrators.
 - SAS Administrators must make CBSD registration information available to the general public, but they must obfuscate the identities of the licensees providing the information for any public disclosures.

Questions?